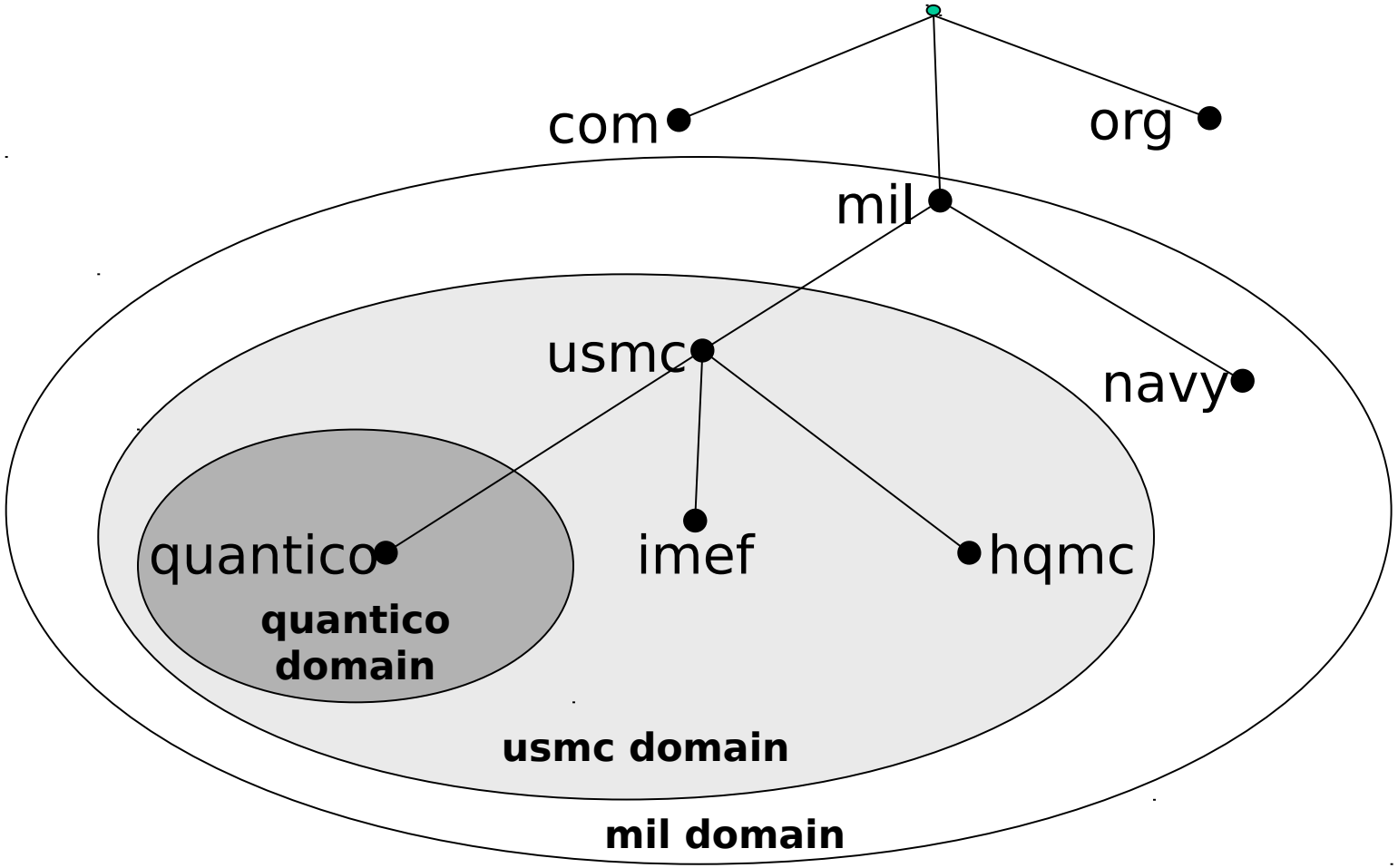
Domain Name Service (DNS)

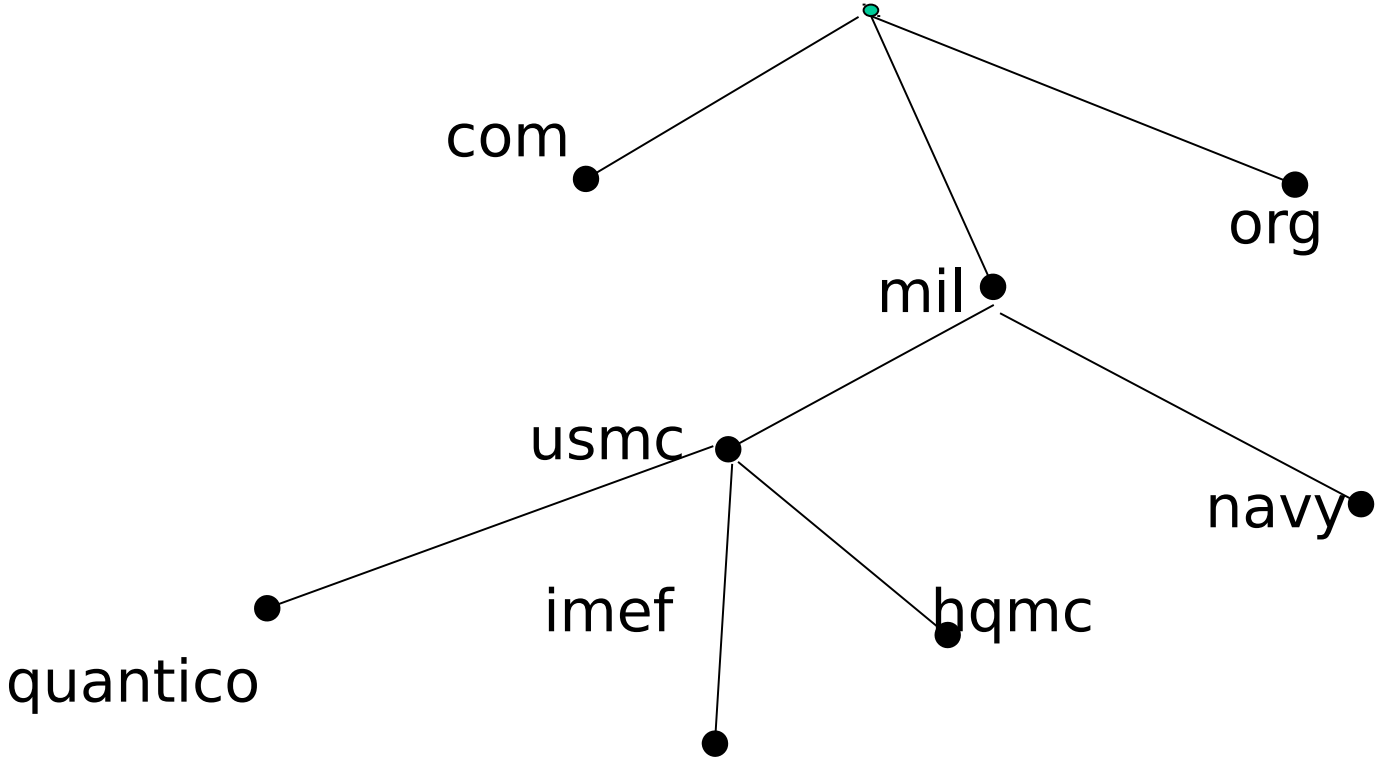
Domain

MSTP


com
org
mil
usmc
navy
quantico
imef
hqmc
quantico domain
usmc domain
mil domain

Subdomains

- Subdomains are completely relative.



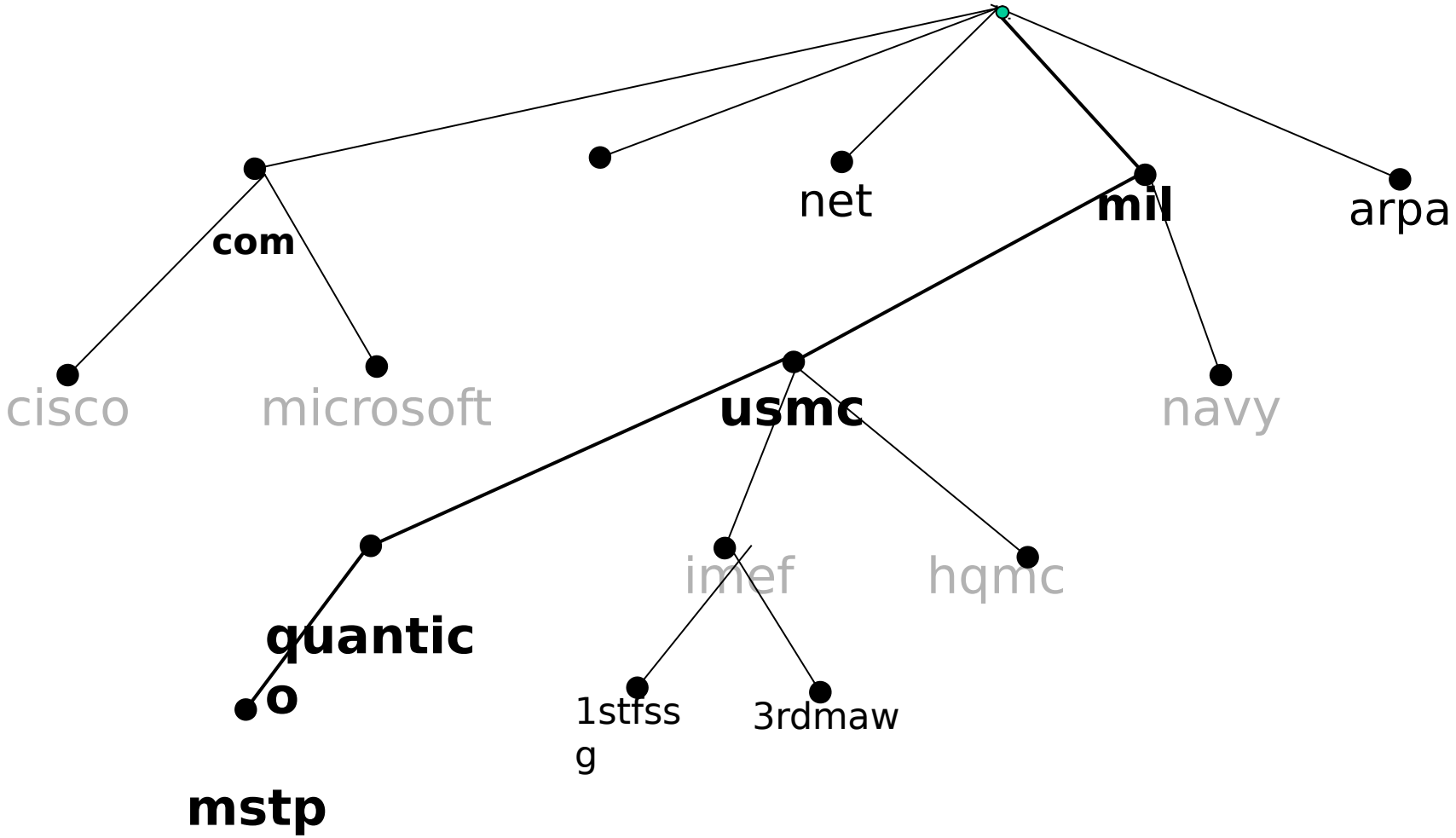
Domain Names

MSTP

- Represent a **node** within the domain name space
- Identify a specific segment of the database.
- Each node has a label that can be up to 63 characters in length.
- The full domain name of any node is the sequence of labels on the path from that node to the root.
- Maximum of 255 characters.
- Valid characters: a-z, A-Z, 0-9, “-” **no underscores!**
- Contact the Marine Corps Network Operations Security Command (MCNOSC).

Domain Names

MSTP



Mstp.quantico.usmc.mil.

Name Servers

MSTP

- The server component of DNS.
- Name servers have complete information about some part of the domain name space, known as a zone.
- Four Types
  - Primary: Start of Authority (SOA) for Zone
  - Master: Any DNS server that receives a request for records
  - Secondary: Receives zone information
  - Caching Only: Holds only cache.dns files

Primary name servers

MSTP

- Primary name servers act as the master database for the organization(s) that they serve.
- The database information is located in plain text files that follow a specific format used by the DNS program.
- These text files can be created, deleted, or modified directly within the primary name server's file system.

Secondary name servers

MSTP

- Provide a backup of the DNS database.
- Spread the load.
- Receive periodical updates to their database from a primary / master name server.
- The Secondary name servers' database cannot be created or modified directly.

Caching-only name servers

MSTP

- Caching-only name servers learn all their database information via queries made to the server.

- Caching-only are not authoritative for any portion of the DNS database.

Resolution

MSTP

- Name servers are capable of providing information about the domain name space.
- The process by which the name servers retrieve information about data is called name resolution.
- A name server can issue a query to a **root name server** for any name in the domain name space, and the root name server will start the name server on its way.

Root Name Servers

MSTP

- Root name servers can at least provide the names and addresses of the name servers authoritative for the top-level domain.

- These top-level name servers can then provide further details regarding the location of authoritative name servers for the domain in question.

Resolution

MSTP

- Simply put, DNS resolution is a matter of converting a workstation's host name into it's corresponding IP address.

- There are primarily two types of resolution:
  - host name to IP address (forward resolution)
  - IP address to host name (reverse resolution)

DNS Zones

MSTP

- Configuration of forward lookup zones and reverse lookup zones
- Forward lookup zone
  - Defined to resolve a name to an IP address
- Reverse lookup zone
  - Defined to resolve IP addresses to names
- The name server can resolve a query only for a zone for which it has authority
- A zone is a database file name that stores entries of the hostname to IP address

DNS and Resource Records

MSTP

- If DNS can not resolve request, it passes it to another name server
- DNS snap-in used to add resource records to the zone database
  - Other types of entries in the zone database file
  - Examples Start of Authority (SOA) or Name Server (NS) records
- DNS SRV records that are required for proper AD operation are
  - GC (Global Catalog)
  - Kerberos
  - LDAP (Lightweight Directory Access Protocol)

Dynamic DNS (DDNS)

MSTP

- Enables automatic updates to zone files by other servers or services
- Prior to 2000, DNS entries were static
- Server is configured with list of authorized servers
  - Secondary name servers, domain controllers, and other servers performing network registration of clients, such as DHCP or WINS

How DDNS Works

MSTP

- Every Windows 2003 computer attempts to register its A record (host record)
  - Provides the name-to-address mapping
- Registers the PTR record (pointer record)
  - Provides address-to-name mapping
- DHCP Client service generates DDNS update on 2003 computers whether or not DHCP client
- DDNS Interacts with DHCP Service to update A and PTR records for DHCP clients and does clean up when lease expires

DNS and Active Directory

MSTP

- Active Directory Integrated DNS

  -Resides in the active directory database (Domain Partition)

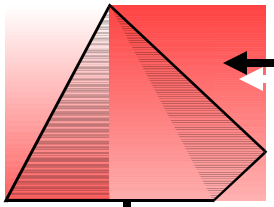
    -When using ADI zones the domain partition will not replicate zone information between zones. You must either setup secondaries of your ADI zone or use delegated zones.

  - Native communication within AD uses TCP/IP and therefore requires DNS for name resolution

  -Service records are dynamically registered in DNS so that clients can contact the appropriate servers in their site

DNS Zone Delegation

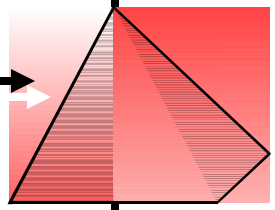
MSTP



USMC.MIL
(Root zone)

Delegated to IIMEF DNS server

IIMEF will create a IIMEF zone



IIMEF zone

(not IIMEF.usmc.mil zone)

Delegated to 2FSSG DNS server

2FSSG will create a 2FSSG zone

2FSSG zone

(not 2FSSG.IIMEF.USMC.MIL zone)

****DNS Zone setup is best done while all servers are still in the same site.****

ADI Zone DNS

MSTP

Standard Zones vs. ADI Zones

- Static
- Single primary zone (read/write copy)
- Centralized control of DNS database and zone transfers
- Not reliant on AD
- Used by non-Windows 2003 DNS servers
- Fault tolerance & load balancing through use of

- Dynamic
- Multiple primaries
- Fault tolerance of primary zone
- Secure zone transfers and DDNS client updates
- Min. zone transfer traffic – depends on AD replication
- Can integrate with standard secondary

Active Directory Design

MSTP

- Don’t make the NETBIOS name and DNS names different
- Name the domain appropriately
- Don’t have conflicts with existing DNS structure
- If you integrate DNS and AD you still need a nominated DNS master
- Larger zones which span sites will generate more replication traffic if they are integrated with AD

Designing the Name Space

MSTP

- Basic emphasis--reduce the number of domains :
- Restrictions
  - Too many GPO’s will result in long log-on times
  - A domain tree cannot be renamed
  - You cannot remove the root forest domain without destroying the entire forest
  - The Schema Admin’s group exists only in the Forest Root Domain
  - Schema Changes are not reversible and cannot be deleted
  - Multiple domains cannot be hosted on a single domain controller
  - The Global Catalog is Global and therefore will replicate data everywhere and doesn’t contain any type of Regional or Site catalog

Designing the Name Space cont…

MSTP

- You should start the design with name space
  - Rough design of the physical design must be in place to finish the name space design
- Geographic, Network, Logical and organizational diagrams of the supported units are required for good planning

Overview Of The Design Process

MSTP

- Stage 1
  - Domain Name Space Design
    - Items to consider :
      - Number of Domains
      - Forest and tree structure
      - Client Naming convention
      - Network as a whole

Stage 1 cont...

MSTP

- Two objectives:
  - Design Active Directory to represent your Units
    - Geographically or Organizational
    - Distributed or Centralized Administration
  - Minimize the use of Domains by utilizing Organizational Units and Sites
    - Each Forest may contain 10 Million objects or more
    - No more than 1 or 2 million per domain is suggested
    - Each Domain can be partitioned using Organizational Units

Stage 1 cont...

MSTP

- Number of Domains
  - Step 1 Three reasons to create domains
    - Isolate Replication
    - Unique Domain Policy
    - NT domain
  - Step 2 Name and Domain Structure
    - Start with the Forest Root
    - Largest Domain left after splitting off the sub domains

Stage 2

MSTP

- Design of the Internal domain structure
  - Use organizational model to determine administrative control and GPO settings
  - Forest Root Domain should be designed first then move on to other trees
    - Consider the Hierarchical structure of your organization

Stage 2 cont...

MSTP

- OU’s should be used to manage your domain structure
  - Delegate administration
  - Easily organized by moving and renaming OU’s
- Designing Users and Groups
  - Groups only contain users or computers
  - User should be placed in the OU to which they correspond

Stage 3

MSTP

- Global Catalog Design
  - Universal groups have an impact on your GC placement
    - GC will be checked for Universal group membership every time a user logs in
  - Queries are much quicker with the GC than with querying the AD

Stage 3 cont...

MSTP

- Global Catalog Design cont...
  - The GC namespace is highly configurable
    - Most objects store at least one property in the GC
    - You can include or exclude any attributes in the GC using the Schema Master Plug-in
    - Decide if objects need to be searchable by the entire forest
    - Determine if you want to exclude any object class from the GC

Design Implications

MSTP

- One DC in each Site for each Domain in that site
- One GC should be placed in each site if your domain is in Native mode
  - Universal groups are expanded upon logon to check your group membership
- How many DC’s should you have
  - Dependant on server specifications, network speed, number of logons at peak time
  - Also dependant on the number of users

Design Implications cont...

MSTP

- Inter-Site Replication
  - Set schedule as needed
    - Ensure that windows match on both ends to ensure that replication can occur
  - Manually setup your site link
  - Let KCC do its job by setting up its own links
  - If you make your site links non-transitive, the KCC will use them but will not automatically create new links as it needs them

Design Implications cont...

MSTP

- IT Section
  - Current Ops
  - Infrastructure
- Finance
  - Pay role
  - Accounts
- Human Resources
- Marketing
- G6
  - Current Ops
  - Infrastructure
- G4
  - Logistics
  - Finance
- G3
- G2

OU’s or Domains?

MSTP